

09/944,788

**RECEIVED
CENTRAL FAX CENTER****AMENDMENTS TO THE CLAIMS:**

NOV 24 2008

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing the alerts into alert classes, both the alerts and the alert classes having a plurality of features, the method comprising the steps of:

- (a) receiving a new alert;
- (b) identifying a set of ~~potentially~~ similar features shared by the new alert and one or more existing alert classes;
- (c) updating a ~~minimum~~ threshold similarity requirement for one or more of the ~~potentially~~ similar features;
- (d) updating a similarity expectation for one or more of the ~~potentially~~ similar features;
- (e) comparing the new alert with the one or more existing alert classes; and either:
 - (f1) associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches; or
 - (f2) defining a new alert class that is associated with the new alert.

2. (Previously Presented) The method of claim 1 further comprising the step (a1) of passing each of the one or more existing alert classes through a transition model to generate a new prior belief state for each of the one or more existing alert classes.

3. (Withdrawn) In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

- (a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;
- (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

09/944,788

- (c) comparing the new alert to one or more alert classes;
- (d) rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value;
- (e) adjusting the comparison by an expectation that certain feature values will or will not match, and either:
 - (f1) associating the new alert with the existing alert class that the new alert most closely matches; or
 - (f2) defining a new alert class that is associated with the new alert.

4. (Withdrawn) In an intrusion detection system that includes a plurality of sensors, each of which generates alerts when attacks or anomalous incidents are detected, a method for organizing the alerts comprising the steps of:

- (a) receiving an alert;
- (b) identifying a set of features that may be shared by the received alert and one or more existing alert classes;
- (c) setting a minimum similarity value for one or more features or feature groups; comparing the new alert to one or more of the alert classes, and either:
 - (d1) defining a new alert class that is associated with the received alert if any feature or feature group that has a minimum similarity value fails to meet or exceed its minimum similarity value; or
 - (d2) associating the received alert with the existing alert class that the received alert most closely matches.

09/944,788

5. (Withdrawn) In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a_method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the method comprising the steps of:

- (a) receiving a new alert;
- (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
- (c) updating a minimum similarity requirement for one or more features;
- (d) comparing the new alert with one or more alert classes, and either:
 - (e1) associating the new alert with the existing alert class that the new alert most closely matches; or
 - (e2) defining a new alert class that is associated with the new alert.

6. (Withdrawn) In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a_method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

- (a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;
- (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;
- (c) comparing the new alert to one or more alert classes;
- (d) rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value, and either:
 - (e1) associating the new alert with the existing alert class that the new alert most closely matches; or
 - (e2) defining a new alert class that is associated with the new alert.

7. (Currently Amended) A computer readable medium containing an executable program for organizing alerts that are generated by a plurality of sensors into alert classes, both the alerts and the alert classes having a plurality of features, where the

09/944,788

program performs the steps of:

- (a) receiving a new alert;
- (b) identifying a set of ~~potentially~~ similar features shared by the new alert and one or more existing alert classes;
- (c) updating a ~~minimum~~ threshold similarity requirement for one or more of the ~~potentially~~ similar features;
- (d) updating a similarity expectation for one or more of the ~~potentially~~ similar features;
- (e) comparing the new alert with the one or more existing alert classes; and either:
 - (f1) associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches; or
 - (f2) defining a new alert class that is associated with the new alert.

8. (Previously Presented) The computer readable medium of claim 7 further comprising the step (a1) of passing each of the one or more existing alert classes through a transition model to generate a new prior belief state for each of the one or more existing alert classes.

9. (Withdrawn) A computer readable medium containing an executable program for organizing alerts that are generated by a plurality of sensors and have a plurality of features, each feature having one or more values, where the program performs the steps of:

- (a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;
- (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

09/944,788

- (c) comparing the new alert to one or more alert classes;
- (d) rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value;
- (e) adjusting the comparison by an expectation that certain feature values will or will not match, and either:
 - (f1) associating the new alert with the existing alert class that the new alert most closely matches; or
 - (f2) defining a new alert class that is associated with the new alert.

10. (Withdrawn) A computer readable medium containing an executable program for organizing alerts generated by a plurality of sensors, where the program performs the steps of:

- (a) receiving an alert;
- (b) identifying a set of features that may be shared by the received alert and one or more existing alert classes;
- (c) setting a minimum similarity value for one or more features or feature groups; comparing the new alert to one or more of the alert classes, and either:
 - (d1) defining a new alert class that is associated with the received alert if any feature or feature group that has a minimum similarity value fails to meet or exceed its minimum similarity value; or
 - (d2) associating the received alert with the existing alert class that the received alert most closely matches.

11. (Withdrawn) A computer readable medium containing an executable program for organizing alerts generated by a plurality of sensors into alert classes, both the alerts and alert classes having a plurality of features, where the program performs the steps:

- (a) receiving a new alert;
- (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
- (c) updating a minimum similarity requirement for one or more features;
- (d) comparing the new alert with one or more alert classes, and either:
 - (e1) associating the new alert with the existing alert class that the new alert most

09/944,788

closely matches; or

(e2) defining a new alert class that is associated with the new alert.

12. (Withdrawn) A computer readable medium containing an executable program for organizing alerts generated by a plurality of sensors and having a plurality of features, each feature having one or more values, where the program performs the steps of:

(a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

(c) comparing the new alert to one or more alert classes;

(d) rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert.

13. (Currently Amended) In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a system for organizing the alerts into alert classes, both the alerts and the alert classes having a plurality of features, where the system comprises:

(a) means for receiving a new alert;

(b) means for identifying a set of ~~potentially~~ similar features shared by the new alert and one or more existing alert classes;

(c) means for updating a ~~minimum~~ threshold similarity requirement for one or more of the ~~potentially~~ similar features;

(d) means for updating a similarity expectation for one or more of the ~~potentially~~ similar features;

(e) means for comparing the new alert with the one or more existing alert classes; and

(f1) means for associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches, or defining a new alert class that

09/944,788

is associated with the new alert.

14. (Previously Presented) The system of claim 13 further comprising (a1) means for passing each of the one or more existing alert classes through a transition model to generate a new prior belief state for each of the one or more existing alert classes.

15. (Withdrawn) In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a system for organizing alerts having a plurality of features, each feature having one or more values, the system comprising:

(a) means for generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;

(b) means for identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

(c) means for comparing the new alert to one or more alert classes;

(d) means for rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value;

(e) means for adjusting the comparison by an expectation that certain feature values will or will not match; and

(f1) means for associating the new alert with the existing alert class that the new alert most closely matches, or defining a new alert class that is associated with the new alert.

16. (Withdrawn) In an intrusion detection system that includes a plurality of sensors, each of which generates alerts when attacks or anomalous incidents are detected, a system for organizing the alerts, the system comprising:

(a) means for receiving an alert;

(b) means for identifying a set of features that may be shared by the received alert and one or more existing alert classes;

(c) means for setting a minimum similarity value for one or more features or feature groups; comparing the new alert to one or more of the alert classes; and

(d1) means for defining a new alert class that is associated with the received

09/944,788

alert if any feature or feature group that has a minimum similarity value fails to meet or exceed its minimum similarity value, or associating the received alert with the existing alert class that the received alert most closely matches.

17. (Withdrawn) In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a system for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, the system comprising:

- (a) means for receiving a new alert;
- (b) means for identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
- (c) means for updating a minimum similarity requirement for one or more features;
- (d) means for comparing the new alert with one or more alert classes; and
- (e1) means for associating the new alert with the existing alert class that the new alert most closely matches, or defining a new alert class that is associated with the new alert.

18. (Withdrawn) In an intrusion detection system that includes a plurality of sensors that generate alerts when attacks or anomalous incidents are detected, a system for organizing alerts having a plurality of features, each feature having one or more values, the system comprising:

- (a) means for generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding feature;
- (b) means for identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;
- (c) means for comparing the new alert to one or more alert classes;
- (d) means for rejecting a match if any feature for which a minimum similarity value has been set fails to meet or exceed the minimum similarity value; and
- (e1) means for associating the new alert with the existing alert class that the new alert most closely matches, or defining a new alert class that is associated with the new alert.

09/944,788

19. (Withdrawn) A method for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the method comprising the steps of:

- (a) identifying a set of potentially similar features shared by a new alert and one or more existing alert classes;
- (b) comparing the new alert to one or more existing alert classes;
- (c) adjusting the comparison by an expectation that certain feature values will or will not match, and either:
 - (d1) associating the new alert with the existing alert class that the new alert most closely matches; or
 - (d2) defining a new alert class that is associated with the new alert.

20. (Currently Amended) A method for organizing alerts into alert classes, both the alerts and the alert classes having a plurality of features, each of the plurality of features having one or more values, the method comprising the steps of:

- (a) receiving a new alert;
- (b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
- (c) updating a similarity expectation for one or more feature values;
- (d) comparing the new alert with the one or more existing alert classes; and either:
 - (e1) associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches; or
 - (e2) defining a new alert class that is associated with the new alert.

21. (Previously Presented) The method of claim 20 further comprising the step (a1) of passing each of the one or more existing alert classes through a transition model to generate a new prior belief state for each of the one or more existing alert classes.

22. (Withdrawn) A method for organizing alerts having a plurality of features, each feature having one or more values, the method comprising the steps of:

- (a) generating a group of feature records for a new alert, each feature record

09/944,788

including a list of observed values for its corresponding features;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

(c) comparing the new alert to one or more alert classes;

(d) adjusting the comparison by an expectation that certain feature values will or will not match, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert.

23. (Withdrawn) A computer readable medium containing an executable program for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, where the program performs the steps of:

(a) identifying a set of potentially similar features shared by a new alert and one or more existing alert classes;

(b) comparing the new alert to one or more existing alert classes;

(c) adjusting the comparison by an expectation that certain feature values will or will not match, and either:

(d1) associating the new alert with the existing alert class that the new alert most closely matches; or

(d2) defining a new alert class that is associated with the new alert.

24. (Currently Amended) A computer readable medium containing an executable program for organizing alerts into alert classes, both the alerts and the alert classes having a plurality of features, each of the plurality of features having one or more values, where the program performs the steps of:

(a) receiving a new alert;

(b) identifying a set of ~~potentially~~ similar features shared by the new alert and one or more existing alert classes;

(c) updating a similarity expectation for one or more feature values;

(d) comparing the new alert with the one or more existing alert classes; and

09/944,788

either:

(e1) associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert.

25. (Previously Presented) The computer readable medium of claim 24 further comprising the step (a1) of passing each of the one or more existing alert classes through a transition model to generate a new prior belief state for each of the one or more existing alert classes.

26. (Withdrawn) A computer readable medium containing an executable program for organizing alerts having a plurality of features, each feature having one or more values, where the program performs the steps of:

(a) generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding features;

(b) identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;

(c) comparing the new alert to one or more alert classes;

(d) adjusting the comparison by an expectation that certain feature values will or will not match, and either:

(e1) associating the new alert with the existing alert class that the new alert most closely matches; or

(e2) defining a new alert class that is associated with the new alert.

27. (Withdrawn) A system for organizing alerts into alert classes, both the alerts and alert classes having a plurality of features, each feature having one or more values, the system comprising:

(a) means for identifying a set of potentially similar features shared by a new alert and one or more existing alert classes;

(b) means for comparing the new alert to one or more existing alert classes;

(c) means for adjusting the comparison by an expectation that certain feature values will or will not match; and

09/944,788

(d1) means for associating the new alert with the existing alert class that the new alert most closely matches, or defining a new alert class that is associated with the new alert.

28. (Currently Amended) A system for organizing alerts into alert classes, both the alerts and the alert classes having a plurality of features, each of the plurality of features having one or more values, the system comprising:

- (a) means for receiving a new alert;
- (b) means for identifying a set of potentially similar features shared by the new alert and one or more existing alert classes;
- (c) means for updating a similarity expectation for one or more feature values;
- (d) means for comparing the new alert with the one or more existing alert classes; and
- (e1) means for associating the new alert with a one of the one or more existing alert classes that the new alert most closely matches, or defining a new alert class that is associated with the new alert.

29. (Previously Presented) The system of claim 28 further comprising (a1) means for passing each of the one or more existing alert classes through a transition model to generate a new prior belief state for each of the one or more existing alert classes.

30. (Withdrawn) A system for organizing alerts having a plurality of features, each feature having one or more values, the system comprising:

- (a) means for generating a group of feature records for a new alert, each feature record including a list of observed values for its corresponding features;
- (b) means for identifying a set of potentially similar features shared by the new alert and one or more existing alert classes that are associated with previous alerts;
- (c) means for comparing the new alert to one or more alert classes;
- (d) means for adjusting the comparison by an expectation that certain feature values will or will not match; and
- (e1) means for associating the new alert with the existing alert class that the

09/944,788

new alert most closely matches, or defining a new alert class that is associated with the new alert.